REMARKS

Claims 1-20 are pending in the patent application.

The Examiner has rejected Claims 1, 5, 12-13, and 15-16 under 35 USC 112 as indefinite. By this amendment, the language of Claims 1, 5, 12, 13, 15 and 16 has been amended pursuant to the telephone interview between the undersigned attorney and Examiner Nalvan. Applicants believe that the amendments address the rejection and recite definite subject matter.

The Examiner has, in paragraphs 7, 11, 14 and 16, stated that Claims 1, 3-4, 7-8, 12 and 15 are rejected under 35 USC 103 as unpatentable over the teachings of Bellovin in view of Aziz; Claims 2, 5-6, 10, 13, 16, and 20 are rejected as unpatentable over Bellovin in view of Aziz and further in view of Mi; Claims 18-20 are rejected as unpatentable over the teachings of Bellovin in view of Aziz and Mi and further in view of Thomlinson; and, Claim 11 is rejected as being unpatentable over the teachings of Thomlinson in view of Aziz, and further in view of Schneier.

Applicants note that there are inconsistencies in the rejections. For example, the Examiner states in paragraph 7

on page 3 of the Office Action that Claims 1, 3-4, 7-8, 12 and 15 are rejected as unpatentable over Bellovin in view of Aziz. The arguments that follow that statement, however, address the language of Claim 9 and 14 which are not expressly rejected. Further, the Examiner cites Thomlinson in paragraphs 9 and 10, and does not cite Bellovin. In addition, the Examiner states in paragraph 16 on page 6 that Claim 11 is rejected as unpatentable over Thomlinson in view of Aziz and Schneier, yet cites Bellovin in paragraph 17. Clarification ***in the form of a NON-FINAL response*** is respectfully requested.

The present invention is a computer program product and method for securely providing data of a content provider to a user without trusting an internet service provider. The present invention allows secure data transfer between a content provider and a user without having the internet service provider participate in the security features, such that transmitted data is always encrypted. In that way, a user could access the internet through any service provider, without sharing any security information with the internet service provider. Similarly, the content provider could securely transmit encrypted data to a trusted user, without

concern that the internet service provider, or other customers of the internet service provider, could access the content provider's data. The security relationship is between the content provider and the user and the claims expressly recite steps for exchanging encryption keys and passwords only between the user and the content provider. By the previous amendments, Applicants have ensured that all of the claims expressly recite that the content provider is not the internet service provider and that the secure transmission is done without trusting the internet service provider.

Claims 5-8, 13, 16 and 19 recite a method, program storage device and means for securely providing data of a content provider through an internet service provider to a user at a client machine without trusting an internet service provider, wherein the content provider and the internet service provider are different entities, the method comprising, when the user accesses a web page of the content provider, downloading an applet from the content provider to the client machine; generating a first key known only to the content provider; generating a second key using the first key and an encryption algorithm requiring a one-time

password; transmitting the second encrypted key for storage at the client machine; and when the user first desires to access the data, the applet requesting the one-time password from the user and, based on correct entry of the one-time password, decrypting said second encrypted key and accessing the data by decrypting an encrypted version of the data at the client machine using the second key. Support for the added features related to downloading and executing the applet is found in the Specification (e.g., at page 6, line 12, and page 7, lines 3-21).

Claims 9-11, 14, 17, and 20, recite a method, program storage device and means for authenticating a user at one client machine seeking access to secure data of a content provider comprising: transmitting g^a and the identity of the user of the one client machine to the content provider node, wherein g and a are random numbers and where a is known only to the client machine, and where g is known to both content provider and the client machine; generating g^b, where b is known to the content provider node but need not be known to the client; encrypting g^b with a one-time password of the user and transmitting g^b to the client machine; at the client decrypting g^b; generating encryption

key K_{ab} using a and g^b; calculating g^(a*b) using the one-time password to decrypt g^b; and encrypting and transmitting g^(a*b) to the content provider, whereby the client machine's knowledge of g^(a*b) authenticates the user to the content provider.

The Examiner has rejected most of the pending claims using the Bellovin reference as the primary reference. The cited teachings of the Bellovin reference, from section 3.1 thereof, detail an encrypted key exchange (EKE) protocol with exponential key exchange. Bellovin teaches that party A picks a random number and calculates an exponential key encrypted with a password that is shared with user B, and then sends the exponential key encrypted with the password to user B. Bellovin does not teach that A generates both a first and a second key and does not teach that A generates the second key using the first key and an encryption algorithm that requires a one-time password. Also, Bellovin does not teach that B stores the second key that it receives from A and directly (i.e., without additional exchange of information between A and B) generates an encryption key for accessing data sent by A. Rather, A and B must further engage in a multi-step exchange of session key K and

challenges under the Bellovin teachings (steps 2-5 in section 3.1) before B would be able to decrypt data sent by A.

The Examiner has acknowledged that Bellovin lacks any mention of a one-time password and has cited the Aziz patent teachings. Applicants contend that Aziz does not provide those teachings which are missing from the Bellovin reference. Aziz does not teach encrypting a second key using a first key and a one time password at one entity and then decrypting the second encrypted key using the one time password and generating an encryption key for decrypting data at the other entity, without any of the additional information exchanges/challenges required by Bellovin.

With regard to Claims 2, 5-6, 10, 13, 16 and 20, the Examiner has further cited the Mi patent in combination with Bellovin and Aziz; and, in rejecting Claim 18-20, the Examiner has cited Mi in combination with Bellovin, Aziz and Thomlinson. The Mi patent is directed to a system and method for using an internet-based caller ID to control client access to an object stored on a server. Under the Mi method, upon receipt of a client request, the server generates a DLL file 407 having a secret key 418 (Col. 7,

lines 23-26) and sends the DLL file with an applet to the client browser (Col. 7, lines 27-33 and 41-44). At the client, the DLL file is executed so that the client uses the same secret key 418 from the DLL file, as well as its processor number 422 which is known to the server (Col. 6, lines 56-67) to calculate a hash value which is returned to the server (Col. 8, lines 4-9 and 32-35). When the server receives the hash value from the client, the server's comparison agent calculates a hash value, compares it to the received hash value, and allows the client access to the data if the two values compare favorably (Col. 8, lines 36-44). For each session, the DLL file will contain a different secret key (Col. 7, lines 26-27 and Col. 8, lines 49-53) which is known to both the server and the client.

The Thomlinson patent, discussed at length in the response to the previous Office Action, provides a system and method for protecting data wherein the service provider is involved in the encryption and authentication process. As expressly stated in Col. 2, lines 12-13 of Thomlinson, "encryption is based on the user's logon password or some other secret supplied during network logon." Applicants reiterate that the security relationship in the Thomlinson

patent is not between a user and a content provider wherein the content provider is a different entity from the service provider. Applicants respectfully assert that one skilled in the art would not look to Thomlinson to modify the Bellovin/Aziz/Mi combination. Further, Applicants disagree with the Examiner's conclusion that Thomlinson teaches the claim features of Claims 18-20 since Thomlinson does not teach the claim features of Claims 2, 6 and 10, from which Claims 18, 19 and 20 respectively depend, that are missing from Bellovin/Aziz/Mi.

Applicants contend that the resulting combination would not obviate the invention as claimed. Since all of Bellovin, Mi and Thomlinson have a key/password that is known to both entities, there is neither a teaching nor a suggestion of generating and using a key that is known to one entity but not known to that other. Moreover, neither reference, alone or in combination with the additionally-cited art, provides for the accessing of data as claimed or the downloading and use of an applet. While Mi may have the processor number known to the server, Mi does not teach or suggest the use of that information for permitting data access only on one client machine.

In rejecting Claim 11, the Examiner has also cited the Applied Cryptography reference for its teachings regarding MAC authentication procedures. Applicants respectfully assert that the reference does not provide the teachings which are missing from the Bellovin and Aziz references. Moreover, Applicants contend that the Examiner has failed to show how the MAC authentication procedures would be integrated into the teachings of the combined references. The Examiner concludes on page 7 that "[b]oth client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security". Applicants disagree with the Examiner's conclusion. Moreover, applying a MAC to Bellovin, alone or in combination with the additionally-cited patents, would not result in the invention as claimed, since none of the cited references teaches or suggests the use of keys not known to the other party, etc.

Applicants respectfully assert that the Examiner has not established a *prima facie* case of obviousness, since the Examiner has not provided prior art which teaches or

suggests all of the claims limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970).

Based on the foregoing remarks, Applicants respectfully request entry of the amendments, reconsideration of the claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

Y. Baransky, et al

By: /Anne Vachon Dougherty/
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910